Compliance Component

DEFINITION	
Name	Configuration Management
Description	Configuration Management is enforcing security configuration settings, monitoring and controlling changes to the established baseline configuration of installed hardware and software.
Rationale	Documenting information system changes and assessing the potential impact of these changes on the security of a system is essential for tracking changes and maintaining continuity.
Benefits	• Provides a comprehensive and continuous documentation of hardware and software changes. • Provides a list of changes to be used when identifying security-related problems. • Provides a back-out road map in case of a malfunction.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Operational Controls
List the Technology Area Name	Hardware & Software Maintenance
List Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	Configuration management involves documentation of the configuration of installed hardware and software at given points in time, systematically controlling changes to the configuration, and maintaining the integrity and traceability of the configuration throughout the lifecycle. The Configuration Management process consists of four phases: 1. Classification – An incident or change is identified and routed to the appropriate organization for resolution. Classification begins when an incident or change is identified. 2. Evaluation – Evaluation begins when the request is received and documented. A technical group validates the request. Then the request is analyzed to determine the extent of its impact. An

	initial solution is identified. 3. Modeling and Testing – A deployment group will develop and document a modeling or testing strategy, configure the evaluation environment, and execute the test. Data from the test will be analyzed and the impact on the overall system will be determined. 4. Implementation – The final solution is approved by management and deployed. Installed software and hardware will continue to be monitored, verified and documented. **Note:** Also refer to Change/Configuration Management Discipline, Systems Management Domain.
Document Source Reference #	NIST Bulletin March 2000 FIPS 200 NIST SP 800-100

Standard Organization			
Name		*Website*	
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	Change, installation, validation, baseline, traceability, modeling, testing, deployment, evaluation.		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			

CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	04/07/2007	*Date Accepted / Rejected*	11/20/07
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			